Does gravitational gossip weigh heavy on your local area network?

Anthony Billups [£],
Reynaldo Castro-Estrada [†],
Wilbert Fern [‡],
Tairi Roque-Urrea [§]
Anthony Tongen[◇]
Ariel Cintrón-Arias [*]

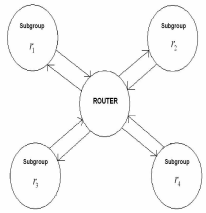
[£] Northeastern University, Boston ,
billups.a@neu.edu
[†] Arizona State University,
Reynaldo.Castro@asu.edu
[‡] Arizona State Univerisity
wfc151986@yahoo.com
[§] Binghamton University,
roque@math.binghamton.edu
[◇] University of Arizona,
tongen@math.arizona.edu
[*] Cornell University,
ariel@cam.cornell.edu

The World Wide Web has proven useful in disseminating information. However, it is extremely difficult to track its spread in such a complex network. One simplification is to model it as a small Local Area Network. Previous work has shown that a gossip-based multicast can be an effective tool for modeling the flow of information on a local area network. We examine the effect of different networks within this mathematical framework. We propose a general mathematical model that incorporates the susceptibility and infectivity of a given machine in a local area network. We also use the concept of proportionate mixing to model the spread of information among heterogeneous patches, where each patch consists of users and non-users of an information router.

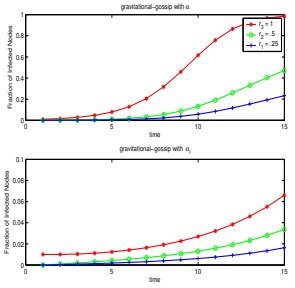
A very interesting idea to model the flow of information is to use a gossip protocol for a subgroup multicast.[?] An example of a multicast process is when someone sends out a mass e-mail to everyone in his or her address book. This framework may be helpful in the study of the spread of information in a small network. The gossip protocol represents the process that information is spread through a system. The protocol idea is to pay close attention to each node in the system and monitor the connections that node makes. This is done so you can have reliable and scalable results for the entire system based on each node. There is a system here in which a person generates some information (the gossip) and sends this gossip via the router to machines registered to receive messages in the local area network. This local area network is broken up into patches based on different rating r. The process by which the gossip is sent by a machine to multiple machines is known as the gossip-based multicast process. Other references about protocols include,[?,?,?,?,?.?] In order to study this idea we use a discrete-time model[?] and a continuous-time proportional mixing. The discrete time model consist of a local area network divided by the rating of each group. For this model we used a very important paramater, *timeout*. The *timeout* specify at what amount of time the gossip is spreading into the local area network.

With the understanding of the division of the network into subgroups, we can examine two parameters of each subgroup. Every machine in the subgroup has an *infectivity* (I) and *susceptibility* (S). These two parameters are based on the machines ability to send and receive gossip. Since every machine in the subgroup has the same rating and timeout, they will also have the same I and S. Let I_i and S_i denote the infectivity and susceptibility for subgroup i, which has rating r_i. Where r_i is the rating of subgroup i. In this model, we refer to a machine that has not received the gossip update as being *susceptible* and a machine that has received the update as *infected*. The model proposed by Jenkis is

$$x_i(t+1) = x_i(t)\exp(-S_i\alpha(t)), \text{for } N_i \text{ large} \qquad (1)$$



Gossip-based Model



Fractions of infected nodes VS time

where N_i is the amount of computer for each subgroup and $x_i(t+1)$ is the fraction of susceptible at time $t+1$. In the numerical simulations, we also considered two other cases for the local area network. For both cases, we calculate the fraction of infections with different values for $\alpha(t)$ and $\alpha_i(t)$. $\alpha(t)$ is the force of infection of the local area network including the patch where the gossip originated. When agossip is sent by a machine, it goes through the router and then it is filtered to all subgroups including the subgroup where the gossip originated. in $\alpha_i(t)$ is the force of infection of the local area network that excludes the patch where the gossip originated. In figure 2 we can see that the fraction of infections with rating 1 can be reduced by 90 percent with $\alpha_i(t)$ getting less infective members in the local area network. This is due to the fact that we have a small number of subgroups. There is a big change if a machine can not spread gossip to machines in its own patch.

In this project we used Castillo-Chavez, C and Song, B[?] model, Continuous-Time Proportional Mixing Model. The idea of this model is having a N population of computers where each computer can communicate with each other in the same neighborhood being a user or non-user of the router. Computers can also communicate to other computers in different neighborhoods while accessing the router. We feel this new model is relevant because it makes sense if everyone does not have access to the router. One example of the model would be if it is expensive to access the router. We assume there are users (U) and non-users (NU) of the router in each of the m different neighborhoods. Divide each group of machines into m neighborhoods according to different rating r_i $1 \leq i \leq m$. Each neighborhood population is divided into subgroups of users and non-users. Assume users and non-users have contact within their own neighborhood. Also, users can also have contacts with other users of another neighborhood. A user from another neighborhood can send a message to the router and the router sends it to users from the m different neighborhoods. The newly infected users can leave the router and infect their own neighborhood, both users and non-users.

Acknowledgements

This research is supported by grants from the Theoretical

Division at Los Alamos National Laboratory, National Science Foundation, National Security Agency, Provost office at Arizona State University, and the Sloan Foundation.

References

[1] Castillo-Chávez, C., Song, B., and Zhang. (2003). An epidemic Model with Virtual Mass-Transpotation: The case of Small-Pox in a Large City. *Bioterrorism Mathematical Modeling Applications in Homeland Security*, (Eds.), Banks, H., and Castillo-Chávez,C., SIAM Frotiers in Applied Mathematics. Springer-Verlag, New York.

[2] Feige, U., Peleg,D., Raghavan, P., and Upfal, E.(1990). Randomized Broadcast in Networks. *Lecture Notes In Computer Science*,450,128-137.

[3] Gibson,D., Kleinberg,J., Raghavan,P. *Inferring Web Communities from Link Topology*. The 9th ACM Conference on Hypertext and Hypermedia,1998.

[4] Gonzalez,T.F.(2003). An efficient algorithm for gossiping in the multicasting communication environment *IEEE Transactions on Parallel and Distributed Systems*, 14, 7, 701-8

[5] Gupta,I.,Kermarrec,A.M., and Ganesh,A.J.(2002). Efficient epidemic-style protocols for reliable and scalable multicast. *Proceedings 21st IEEE Symposium on Reliable Distributed Systems*,180-9

[6] Jenkins, K., Hopkinson, K., and Birman K.Ł(2001). Reliable Group Communication with Subgroups. *IEEE International Workshop on Applied Reliable Group Communication within the International Conference on Distributed Computing Systems 16-19 of April 2001, Pheonix, USA.*

[7] Karp,R.,Schindelhauer,C.,Shenker,S., and Vocking,-B.(2000). Randomized rumor spreading. *Proceedings 41st Annual Symposium on Foundations of Computer Science*,565-74.